[Scope of Claim for a Patent]

[Claim 1]

A user authentication system of authenticating a user of a client-server distribution network system as a legitimate user qualified to request a service from a server, in a client-server distribution network system having a terminal equipment of requesting the service in accordance with the instruction of the user, the server of providing the service and a network connecting the terminal equipment and the server, characterized by comprising:

a plurality of ciphering/deciphering means of each executing the ciphering/deciphering processing corresponding to different security levels;

a security level storage means of storing the security level of each user and each terminal equipment designated in advance; and

a ciphering/deciphering means selecting means of selecting a ciphering/deciphering means corresponding to the security level stored in the security level storage means from a plurality of the ciphering/deciphering means at the time of executing the ciphering/deciphering processing.

[Claim 2]

A user authentication system of authenticating a

user of a client-server distribution network system as a legitimate user qualified to request a service from a server, said client-server distribution network system having a terminal equipment of requesting the service in accordance with the instruction of the user, the server of providing the service and a network connecting the terminal equipment and the server, characterized by comprising:

a plurality of key management means of each executing the key management corresponding to different security levels;

a security level storage means of storing the security level of each user and each terminal equipment designated in advance; and

a key managing means selecting means of selecting a key managing means corresponding to the security level stored in the security level storage means from a plurality of the key managing means at the time of key acquisition.

[Detailed Description of the Invention]

[0001]

[Industrial Field of the Invention]

This invention relates to a user authentication system for a client-server distribution network system.

[0002]

[Prior Art]

In the prior art, Kerberos developed by Athena Project of MIT is widely known as an authentication system for the client-server distribution network system (See Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller, "Kerberos: An Authentication Service for Open Network systems" USENIX Winter Conference, February 9-12, 1988, Dallas, Texa, or John T. Kohl, "The Evolution of Kerberos Authentication Service" Spring, 1991, EurOpen Conference, Tromso, Norway).

[0003]

Kerberos provides a user authentication function based on a reliable third party employing DES as an ciphering algorithm. First, the Kerberos user authentication system is explained.

[0004]

Fig. 1 shows an outline of a client-server distribution network system. In the drawing, numeral 1 designates a client computer (hereinafter referred to as the terminal equipment) requesting a service in accordance with a user instruction, numeral 2 s server computer (hereinafter referred to simply as the server) providing the service, numeral 3 an authentication server computer (hereinafter referred

to simply as the authentication server) for authenticating a user of the terminal equipment 1 as a legitimate user (a user qualified to request a service from the server) for the server 2, and numeral 4 a network connecting the terminal equipment 1, the server 2 and the authentication server 3.

[0005]

In the Kerberos user authentication system, the terminal equipment 1 includes a means of creating a private key Ku of the user constituting a DES key from the password designated by the user, a means of ciphering/deciphering a message in accordance with the DES algorithm and a means of acquiring the time. The server 2 includes a means of holding a private key Ks of the server constituting a DES key indicating the identity of the server 2, a means of ciphering/deciphering a message in accordance with the DES algorithm, and a means of acquiring the time. The authentication server 3, on the other hand, includes a means of holding both the private key Ku of the user and the private key Ks of the server 2 constituting the DES keys and a means of creating a session key constituting a DES key shared by the terminal equipment 1 and the server 2.

[0006]

The Kerberos user authentication system is explained below step by step. In the process, assume that E(Kx, X) indicates the value obtained by ciphering the value X with the key Kx, D(Kx, X) the value obtained by deciphering the value X with the key Kx, and X||Y the value obtained by connecting X and Y.

[0007]

(Step 1) In response to a user instruction, the terminal equipment 1 requests a session key Kus, from the authentication server 3 through a network 4, used for proving to the server 2 that the user is a legitimate one.

[0008]

(Step 2) In the case where the request from the terminal equipment 1 is based on the instruction from the user of which the authentication server 3 holds the private key, the authentication server 3 creates the session key Kus, and ciphers the session key Kus in accordance with the DES algorithm with the private key Ku of the user. At the same time, the session key Kus is ciphered also with the private key Ks of the server 2 in accordance with the DES algorithm. These ciphered session keys E(Ku, Kus) and E(Ks, Kus) are sent to the terminal equipment 1 through the network 4.

[0009]

(Step 3) The session key E(Ku, Kus) ciphered by the private key Ku of the user and sent from the authentication server 3 through the network 4 is deciphered by the terminal equipment 1 in accordance with the DES algorithm with the private key Ku of the user created from the password input from the user, thereby obtaining the session key Kus for the server 2.

[0010]

(Step 4) The terminal equipment 1 acquires the present time T1, ciphers it in accordance with the DES algorithm with the session key Kus, and sends it to the server 2 through the network 4 together with the session key E(Ks, Kus) received from the authentication server 3.

[0011]

(Step 5) The server 2 deciphers the received session key E(Ks, Kus) with his/her private key Ks in accordance with the DES algorithm and thereby obtains the session key Kus. With this key Kus, the ciphered time E(Kus, T1) sent from the terminal equipment 1 is deciphered in accordance with the DES algorithm thereby to obtain the time T1.

[0012]

Thus, the present time T2 is acquired and compared with time T1. In the case where T1 plus 5

minutes is smaller than T2, the server 2 determines that the user who has instructed the terminal equipment 1 to request a service is a legitimate user, and begins to provide the service. Otherwise, the server 2 determines that the user is not a legitimate one and refuses to provide the service.

[0013]

[Problem to be Solved by the Invention]

In this Kerberos, as described above, the ciphering/deciphering is conducted always in accordance with the DES algorithm and no other ciphering algorithm cannot be selected in the course of user authentication. In the actual system, however, it is sometimes desired to employ a user authentication system different in security level (safety) for each user or terminal equipment depending on the system configuration or the conditions on which the service is provided.

[0014]

In the case of the in-house bulletin board service, for example, a user authentication system is desired which gives priority to the response time at the sacrifice of low security level. In the personnel system, on the other hand, it is desired to employ a user authentication system very high in security level.

In such a case, the user authentication for the bulletin board service may use the CBC mode of FEAL-8 as a ciphering algorithm, while the user authentication for the personnel system may use the CBC mode of FEAL-32X as a ciphering algorithm. In this way, a ciphering algorithm suitable for the required security level is desirably selected for each user or each terminal equipment in the same system.

[0015]

In similar fashion, with regard to the means of managing the private key indicating the user identity, Kerberos has only the means of automatically creating the private key from the password stored by the user. Against the password attack from the hacker, therefore, the safety of at most about the same level as the conventional user authentication method of password input type can be provided.

[0016]

At present, however, a device of highly safety such as an IC card can be used, and in the case where a high security level is required, this device, though expensive, is used, while a means is used to automatically create the private key from a password like Kerberos in the case where a high security is not required. In this way, it is desirable to select a

private key managing means suitable for the required security level for each user or each terminal equipment in the same system.

[0017]

An object of this invention is to provide a user authentication system in which the ciphering/deciphering means having different security levels meeting the requirement of the user or the terminal equipment can be selected within the same system.

[0018]

Another object of the invention is to provide a user authentication system in which the private key managing means having different security levels meeting the requirement of the user or the terminal equipment can be selected within the same system.

[0019]

[Means for Solving the Problem]

In order to achieve the objects described above, according to claim 1 of the invention, there is proposed a user authentication system of authenticating a user as a legitimate user qualified for issuing a service request to a server in a client-server distribution network system including a terminal equipment of requesting the service in

accordance with a user instruction, a server of providing the service and a network for connecting the terminal equipment and the server, the user authentication system comprising a plurality of ciphering/deciphering means of each executing the ciphering/deciphering processing in accordance with different security levels, a security level storage means of storing the security level for each user or each terminal equipment designated in advance, and an ciphering/deciphering means selecting means of selecting an ciphering/deciphering means corresponding to the security level stored in the security level storage means from a plurality of the ciphering/deciphering means at the time of the ciphering/deciphering processing.

[0020]

According to claim 2, there is provided a user authentication system of authenticating a user as a legitimate user qualified for issuing a service request to a server in a client-server distribution network system including a terminal equipment of requesting the service in accordance with a user instruction, a server of providing the service and a network for connecting the terminal equipment and the server, the user authentication system comprising a

plurality of key management means of each executing the key management process in accordance with different security levels, a security level storage means of storing the security level for each user or each terminal equipment designated in advance, and a key managing means selecting means of selecting a key managing means corresponding to the security level stored in the security level storage means from a plurality of the key managing means at the time of key acquisition.

[0021]

[Operation]

According to claim 1 of the invention, in executing the ciphering/deciphering processing using the private key of a user with the authentication of the particular user, the ciphering/deciphering means corresponding to the security level of each user or terminal equipment stored in the security level storage means can be selected from a plurality of the ciphering/deciphering means by the ciphering/deciphering means selecting means. Thus, the user authentication is possible in accordance with the security level for each user or terminal equipment.

[0022]

Also, according to claim 2, in acquiring the

private key of a user with the authentication of the user, a key managing means corresponding to the security level of each user or each terminal level stored in the security level storage means can be selected by the key managing means selecting means from a plurality of the key managing means. Thus, the user authentication is possible in accordance with the security level for each user or terminal equipment.

[0023]

[Embodiments]

Embodiments of the invention are explained below with reference to the drawings. In this case, an example of application of this invention to a 5-pass authentication method using a reliable third party based on the conventional key ciphering algorithm is explained as described in "6.2 Five pass authentication" of ISO/IEC 9798-2 "Information technology - Security techniques - Entity authentication mechanism; Part 2; Entity authentication using symmetric techniques".

[0024]

An outline of the client-server distribution network system according to this embodiment is similar to the one shown in Fig. 1.

[0025]

Fig. 2 shows a terminal equipment according to this embodiment. In the drawing, numeral 11 designates a communication means, numeral 12 a user information acquisition means, numeral 13 an authentication means, numerals 14-1, 14-2, …,14-m ciphering/deciphering means, numerals 15-1, 15-2, …, 15-n key managing means, numeral 16 a security level storage means, numeral 17 a ciphering/deciphering means selecting means, and numeral 18 a key managing means selecting means.

[0026]

The communication means 11 is connected to the network 4 and conducts communication with the server 2 and the authentication server 3. The user information acquisition means 12 acquires the user identifier from the user. The authentication means 13 executes the authentication method based on ISO 9798-2.

[0027]

The ciphering/deciphering means 14-1 to 14-m each execute the ciphering/deciphering processing in accordance with different security levels, and have various different algorithms such as FEAL and DES and various different use modes of the ciphering algorithms such as EBC mode, CBC mode, CFB mode and OFB mode. The key managing means 15-1 to 15-n execute

the management of the private key corresponding to different security levels, and have different types of hardware such as IC card, PCMCIA card and ROM.

[0028]

The security level storage means 16 stores the security level of each user or terminal equipment designated in advance. The ciphering/deciphering means selecting means 17 selects, out of the ciphering/deciphering means 14-1 to 14-m, the one corresponding to the security level stored in the security level storage means 16, based on the request from the authentication means 13. The key managing means selecting means 18 selects, out of the key managing means 15-1 to 15-n, the one corresponding to the security level stored in the security level storage means 16 based on the request from the authentication means 13.

[0029]

Fig. 3 shows the sequence of messages exchanged among the terminal equipment 1, the server 2 and the authentication server 3 according to this embodiment. The authentication operation according to this embodiment is explained below.

[0030]

First, the terminal equipment 1 acquires the user

identifier IDu using the user information acquisition means 12. Next, the user identifier IDu is delivered to the authentication means 13, which in turn creates a message M1 from the user identifier IDu and the random number Ru generated, and sends the message M1 to the server 2 through the communication means 11.

[0031]

The server 2 generates a message M2 from the server identifier IDs, the random number Rs1 generated and IDu and Ru in the message M1, and sends it to the authentication server 3.

[0032]

The authentication serve 3 acquires the private keys Ku, Ks in registration from the user identifier IDu and the server identifier IDs, and further generates the session key Ksu shared by the terminal equipment 1 and the server 2. Next, the session key Ksu, the random number Ru sent from the terminal equipment 1 and the random number Rs1 sent from the server 2 are coupled to each other. Further, they are ciphered by the private key Ku of the user and the private key Ks of the server 2. In this way, the message M3, i.e. E(Ku, Ru||Ksu) and E(Ks, Rs1||Ksu) are generated and sent back to the server 2.

[0033]

The server 2 deciphers E(Ks, Rs1||Ksu) constituting a part of the message M3 with the private key Ks of the server 2, and acquires the random number Rs1 and the session key Kus. The random number thus acquired and the random number sent in the message M2 are collated with each other, and in case of coincidence, it is determined that the message M3 is a response from the right authentication server 3, and the subsequent operation is continued.

[0034]

Next, the server 2 generates a new random number Rs2, which is coupled with the random number Ru sent in the message M1 from the terminal equipment 1, and ciphered by the session key Kus. With the remaining portion of the message M3, the message M4, i.e. E(Ku, Ru||Ksu), E(Ksu, Ru||Rs2) are generated and sent to the terminal equipment 1.

[0035]

The terminal equipment 1 receives the message M4 through the communication means 11 and delivers it to the authentication means 13. The authentication means 13, in order to decipher the part E(Ku, Ru||Ksu) of the message M4 sent from the authentication server 3, first requests the key management selecting means 18 to acquire the private key Ku of the user.

[0036]

The key managing means selecting means 18 makes inquiry to the security level storage means 16 about the security level. The security level storage means 16 notifies the security level stored therein to the key managing means selecting means 18. The key managing means selecting means 18, in accordance with the security level notified from the security level storage means 16, selects an appropriate one of the key managing means 15-1 to 15-n, acquires the private key Ku of the user through the key managing means and delivers it to the authentication means 13.

[0037]

Next, the authentication means 13 requests the ciphering/deciphering means selecting means 17 to decipher E(Ku, Ru||Ksu) by the private key Ku of the user obtained from the key managing means selecting means 18. The ciphering/deciphering means selecting means 17 makes an inquiry to the security level storage means 16 about the security level. The security level storage means 16 notifies the security level stored therein to the ciphering/deciphering means selecting means 17.

[0038]

The ciphering/deciphering means selecting means

17, in accordance with the security level notified from the security level storage means 16, selects an appropriate one of the ciphering/deciphering means 14-1 to 14-m, and using the particular ciphering/deciphering means, deciphers E(Ku, Ru||Ksu). Thus, the random number Ru and the session key Kus are acquired and delivered to the authentication means 13.
[0039]

The authentication means 13 collates the random number acquired from the ciphering/deciphering means selecting means 17 with the random number sent in the message M1, and in case of coincidence, determines that the message M4 is a a response to the right authentication server and continues the subsequent operation.
[0040]

Next, with the session key Kus obtained, the ciphering/deciphering means selecting means 17 is requested to decipher the part E(Ksu, Ru||Rs2) of the message M4 sent from the authentication server 3. The ciphering/deciphering means selecting means 17 makes an inquiry to the security level storage means 16 about the security level. The security level storage means 16 notifies the security level stored therein to the ciphering/deciphering means selecting means 17.

[0041]

The ciphering/deciphering means selecting means 17, in accordance with the security level notified from the security level storage means 16, selects an appropriate one of the ciphering/deciphering means 14-1 to 14-m and using the particular ciphering/deciphering means, deciphers E(Ksu, Ru||Rs2). Thus, the random number Ru and the random number Rs2 are acquired and delivered to the authentication means 13.

[0042]

The authentication means 13 collates the random number Ru acquired from the ciphering/deciphering means selecting means 17 with the random number sent in the message M1, and in case of coincidence, determines that the message M4 is a response from the right server 2, and continues the subsequent operation.

[0043]

Next, with the session key Kus obtained, the authentication means 13 requests the ciphering/deciphering means selection means 17 to cipher the random number Rs2 and the random number Rsu sent from the server 2. The ciphering/deciphering means selecting means 17 makes an inquiry to the security level storage means 16 about the security

level. The security level storage means 16 notifies the security level stored therein to the ciphering/deciphering means selecting means 17.

[0044]

The ciphering/deciphering means selecting means 17, in accordance with the security level notified from the security level storage means 16, selects an appropriate one of the ciphering/deciphering means 14-1 to 14-m and using the particular ciphering/deciphering means, ciphers the random numbers Rs2 and Ru, and delivers them to the authentication means 13.

[0045]

The authentication means 13 sends the obtained E(Ksu, Rs2||Ru as a message M5 to the server 2 through the communication means 11.

[0046]

The server 2 deciphers the message M5 sent thereto by the session key Kus, and acquires the random numbers Ru, Rs2. The acquired random number Rs2 is collated with the random number sent in the message M4, and in case of coincidence, it is determined that the message M5 is a response from the right terminal equipment 1.

[0047]

[Effects of the Invention]

As described above, according to claim 1 of the invention, when carrying out the ciphering/deciphering processing using the private key of a user for authentication of the user, a ciphering/deciphering means corresponding to the security level of each user or terminal equipment stored in the security level storage means can be selected by a plurality of the ciphering/deciphering means selecting means, and the authentication of a user corresponding to the security level of each user or terminal equipment can be performed. Thus, an optimum security meeting the conditions on the part of the user and the terminal equipment including the cost, performance and place of installation of the terminal equipment is realized.

[0048]

Also, according to claim 2 of the invention, when acquiring the private key of a user for authentication of the user, a key managing means corresponding to the security level of each user and terminal equipment stored in the security level storage means can be selected from a plurality of key managing means by the key managing means selecting means, and the user authentication corresponding to the security level of each user and terminal equipment can be performed.

Thus, an optimum security is realized meeting the conditions on the part of the user and the terminal equipment including the cost, the performance and the place of installation of the terminal equipment and the presence or absence of the IC card unit.

[Brief Description of Drawings]

[Fig. 1]

A configuration diagram showing an outline of a client-server distribution network system.

[Fig. 2]

A configuration diagram showing a terminal equipment according to an embodiment of the invention.

[Fig. 3]

A diagram showing the sequence of the message exchanged among the terminal equipment, the server and the authentication server.

[Description of Reference Numerals]

1 … Terminal equipment, 2 … Server, 3 … Authentication server, 4 … Network, 11 … Communication means, 12 … User information acquisition means, 13 … Authentication means, 14-1 to 14-m … Ciphering/deciphering means, 15-1 to 15-n … Key managing means, 16 … Security level storage means, 17 … Ciphering/deciphering means selecting means, 18 … Key managing means selecting means.

Fig. 1

①: Private key

②: Authentication server

③: Network

④: Session key

⑤: Server

⑥: Terminal equipment

Fig. 2

①: Network

11: Communication means

12: User information acquisition means

13: Authentication means

14-1 to 14-m: Ciphering/deciphering means

15-1 to 15-n: Key managing means

16: Security level storage means

17: Ciphering/deciphering means selecting means

18: Key managing means selecting means

Fig. 3

①: Terminal equipment

②: Server

③: Authentication server

④: Message M1

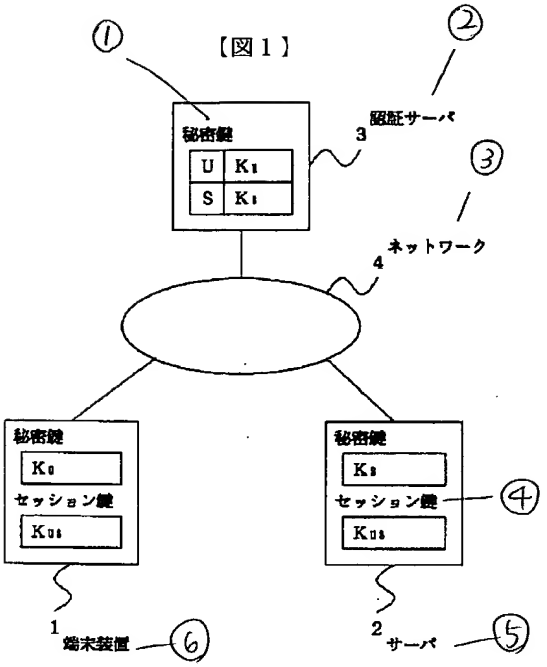
⑤: Message M2

⑥: Message M3

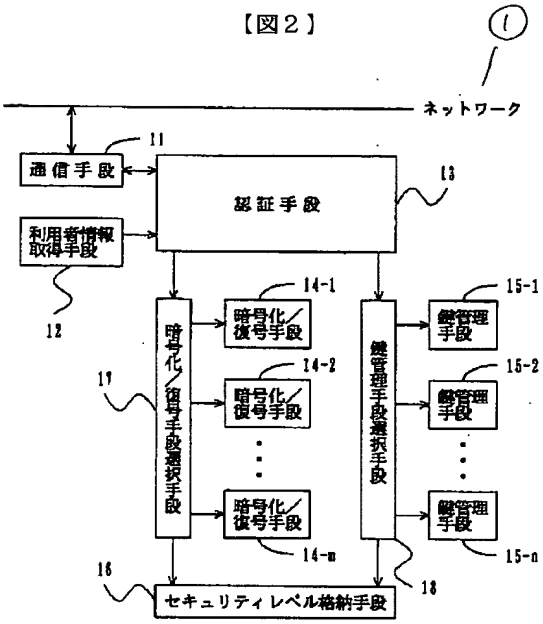
⑦: Message M4

⑧: Message M5

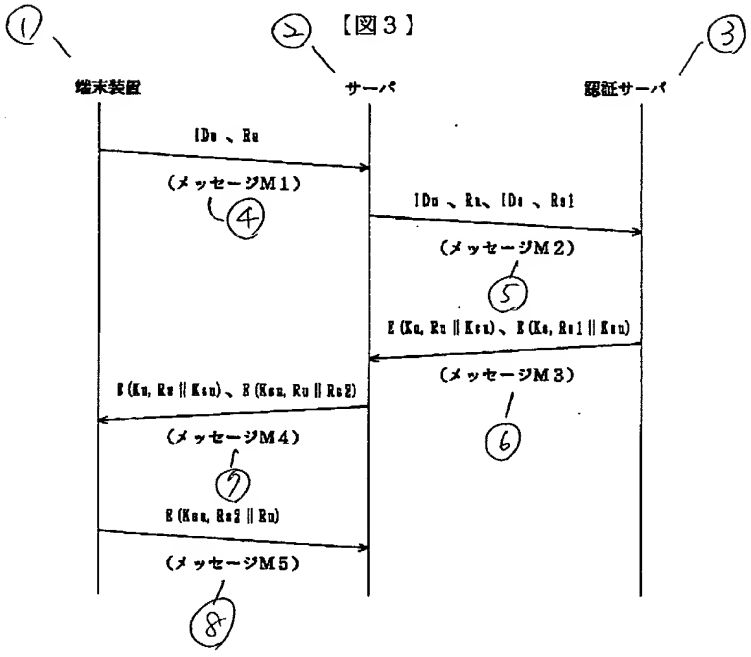
【図１】



【図２】



【図３】



フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ	9/12				
// Ｇ０６Ｆ	1/00	３７０			